

State of Alabama
Email Policy

Table of Contents

1.	Purpose.....	4
2.	Scope.....	5
3.	Policy	6
3.1	General Notice:	6
3.2	Rules for Using State E-mail	6
3.3	Roles and Responsibilities	8
3.4	Access to State E-mail System:	8
3.5	Guidance for Agencies.....	8
3.5.1	Use of e-mail for personal communications	8
3.5.2	Deletion of personal and transitory messages.....	9
3.5.3	Format and content of messages	9
3.5.4	Records Retention.....	9
3.5.5	Records Disposal	9
3.6	Legal requirements.....	9
3.7	Best practices	9
3.8	Personal Use.....	10
3.9	System Monitoring.....	10
3.10	Disclaimer	10
4.	References.....	11
5.	Declaration.....	12

1. Purpose

The purpose of this policy is to ensure the proper use of the state of Alabama's email system and make users aware of what the state deems as acceptable and unacceptable use of its email system. The state reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

2. Scope

Electronic mail (e-mail) enables the user to send and receive messages, make appointments, or coordinate work schedules rapidly and efficiently. The advantages of e-mail have caused a rapid growth in the use of this technology. With the rapid expansion of e-mail throughout Alabama State agencies, more data are being transmitted between employees without the use of traditional paper documents. This trend increases the possibility of State records being lost before completing their retention cycle, and the messages being subpoenaed for use in litigation. Records contained within the e-mail system need to be identified and controlled in the same manner as any other record.

This policy shall apply to all State of Alabama employees whether full-time, part-time, or contract as well as all individuals contracted to perform work for the State. Each agency may develop its own e-mail policy provided that, at a minimum, all provisions set forth in this policy are contained in its policy. In such a case, the more restrictive e-mail policy shall take precedence.

Users are cautioned that the use of e-mail and attachments thereto may create the need to preserve other forms of data, such as graphics files, digital photographs, sound files and video clips. When using these data forms in conjunction with the e-mail system, please consult your agency's policies or computer specialist for advice on the use and preservation of such data.

Public records, including those created in e-mail, are the property of the State of Alabama.

3. Policy

3.1 *General Notice*

Electronic mail is an electronic file that is transmitted to other computer users. When transmitted to a recipient, electronic mail may create the sender's electronic file in the recipient's computer system. Deleting electronic mail does not ensure erasure of all copies of the file. Copies of deleted files may be stored remotely for long periods of time, and can be accessed and disclosed. Therefore, employees should not expect their electronic communications to be private, and should not use electronic mail for communications not intended for disclosure to third parties. Although the contents of business-related electronic mail are subject to the same rules of legal privilege as other forms of communication and record keeping, employees should treat the electronic mail system as a shared file system, with the expectation that messages sent, received or stored in the system (including individual hard disks) may be subject to access, monitoring and disclosure. Employees should be aware that documents sent via e-mail for official business or as evidence of official acts may constitute official records of the State.

Nothing in this policy should be construed to waive any claim of privilege or confidentiality for the contents of electronic mail available to the State or to require public disclosure of electronic communications.

3.2 *Rules for Using State E-mail*

1. Messaging system not a storage system. The State's e-mail system is designed for communication by written message. It is not and should not be used as a document storage or management system.
2. Official Business. The State's e-mail systems are for official business **only**. All messages sent or received on the system are the property of the State of Alabama.
3. Expectation of Privacy. Employees should not expect e-mail messages in their basic form to be private. E-mail is no more immune from unauthorized interception than any other electronic communication; therefore agencies should consider encryption of sensitive information or consider alternative means of communication. Each agency must have a plan for separating out confidential material sent by e-mail, or have a policy that confidential materials and communications will not be sent through this medium.
4. E-mail Account. E-mail accounts, and the e-mail messages contained within these accounts, are important to the business functions of an individual State agency. As such, the messages and e-mail accounts are the property of the State of Alabama. In the event of any employee termination or interagency transfer, the employee's e-mail account shall remain with the originating agency. All messages may be reviewed and redirected to the employee's successor or otherwise purged of agency-specific content

as appropriate.

5. Improper uses. The use of the e-mail system to transmit data which is disparaging or harassing to individuals or groups will not be tolerated. Types of data include: writings, drawings or any other form that is degrading or harassing to others based on, but not limited to, race, age, origin, sex, disability, religion or political beliefs, including “jokes.” E-mail may not be used for personal commercial ventures, religious or political causes, endorsement of candidates, or outside organizations.
6. Security. To ensure system integrity and security, each individual must protect his system password from disclosure to others. Please refer to the *State of Alabama Password Guidelines* for guidance in addition to that which follows:
 - **Passwords may not be shared.**
 - **Passwords may not be cached.** For employees, this means never using the “Remember Password” feature of any application (for example Outlook, Outlook Express, Outlook Web Access).
 - The use of passwords to gain access to the computer system or to secure specific files does not provide users with an expectation of privacy in the respective system or document.
 - Passwords must never be stored in readable form in batch files, automatic login scripts, software macros, or terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover them.
 - **Passwords must be changed every 60 days.** Passwords cannot be reused. History is kept for 12 passwords
 - User must use “**strong**” password standards. Please reference *State of Alabama Password Guidelines*.
7. Copies and dissemination. E-mail can be copied and forwarded to numerous individuals. Copies of an e-mail may be retained by persons unknown to the author long after the intended function has been completed. Both recipients and transmitters need to protect data sent on the system from unauthorized alteration and deletion.
8. Copyright violations. The ability of various e-mail systems to include attachments enables the users to forward additional data to other users. The ease of transmitting attachments places the burden of protecting copyrighted material on the transmitter. Protection of copyrights requires the user to make, to the greatest degree possible, a determination of authorship of any data utilized. All copyright laws apply equally to e-mail systems.
9. Etiquette. Use of e-mail etiquette should be observed at all times. Employees represent the State of Alabama and should act in a professional manner at all times.
10. Viruses and E-mail. Simply reading a text based e-mail can spread a virus to your computer. This is a relatively new development. Viruses can also be hidden in attachments to mail messages. There is risk from opening attached files to the e-mail message, especially executable files. In addition, other types of file attachments can

pose a risk, such as MS-Word documents, Excel spreadsheets, and similar files used by applications that use macros, because these files can be infected with a macro virus. If you receive any unsolicited e-mail from unknown sources or untrusted documents or executable programs via an e-mail attachment, the file should be saved to the local hard drive and scanned with an anti-virus scanning product (with the latest virus signatures or definitions installed) before the file is opened or run. The IT person should be contacted for assistance. Be aware that this is not an absolute guarantee that the contents of the file are safe, but it will check for any viruses or malicious code that the scanning software can detect. If there is any doubt (especially if the e-mail was sent from an unknown source), deleting unsolicited messages with all attached files is the safest thing to do.

Users are requested not to spread unconfirmed warnings about viruses. If you receive an invalidated warning, do not pass it to others; pass it to your systems administrator to validate first.

3.3 Roles and Responsibilities

1. **Agency policies:** Agency management should create and distribute an email policy that contains the statewide and any additional agency-specific policies appropriate to the agency's business needs. In all cases, the most restrictive policy shall take precedence.
2. **Agency responsibilities:** Agencies are responsible for assisting users to manage their records by providing technical means and advice to implement records management policies.
3. **User responsibilities:** End users are responsible for managing the email messages they receive and for properly identifying, classifying, retaining, and disposing of messages—as well as arranging for transferring email records to their successors or archival repository—in accordance with statewide and agency policies.

3.4 Access to State E-mail System:

Employees of the State are granted access to the e-mail system to carry out their assigned duties. System privileges to non-employees shall be granted only with approval of the agency director or his designee. Access to the e-mail system may be terminated at any time if it has been determined access is no longer needed or there has been abuse of the system.

3.5 Guidance for Agencies

3.5.1 Use of e-mail for personal communications

Agencies may permit employees to use e-mail for occasional and incidental personal communications--the same way employees use phones--or may prohibit any personal use.

3.5.2 Deletion of personal and transitory messages

An agency that permits limited personal use of e-mail should direct workers to delete any message that is not a state business record, immediately after reading the message. E-mail users should also be instructed to delete duplicates and messages of limited communicative value.

3.5.3 Format and content of messages

Agencies should specify basic e-mail format elements for employees to make identification clear for records purposes. In fact, agencies can specify functional records-naming conventions to help employees manage records. Agencies can also provide guidelines for appropriate language and content of messages, since workers might treat the medium informally, even though it creates a public record.

3.5.4 Records Retention

Agencies should inform e-mail users about common records series and their retention periods. Agencies should also advise employees how to retain records for appropriate periods to ensure access. Due to the difficulties of retaining and accessing long-term records in e-mail systems, agencies should provide solutions for managing e-mail records in electronic form. As an interim measure in the absence of an adequate technical solution, agencies can also specify that some or all long-term records should be printed out and retained in paper files. The State standard for e-mail retention is 90 days.

3.5.5 Records Disposal

Agencies should advise e-mail users how to dispose of records according to approved retention policies for records of like content and value in other media. Agencies can also specify the minimum frequency for end-user destruction of e-mail records in the normal course of business, or the central e-mail administrator can establish a method for doing so.

3.6 Legal requirements

The following rules are required by law and will be strictly adhered to. It is **prohibited** to:

- Send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an email of this nature, you must promptly notify your supervisor.
- Send unsolicited commercial email messages.
- Forge or attempt to forge email messages.
- Disguise or attempt to disguise your identity when sending mail.
- Send email messages using another person's email account.
- Intercept e-mail messages not destined for the subject

3.7 Best practices

The state considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service. Users should take the same care in drafting

an email as they would for any other communication. Therefore the state wishes users to adhere to the following guidelines:

- Writing emails:
 - Write well-structured emails and use short, descriptive subjects.
 - Signatures must include the sender's name, job title and agency name. A disclaimer must be added underneath the sender's signature (see Disclaimer)
 - Do not send unnecessary attachments; and compress attachments larger than 200K before sending them.
 - Do not write emails in all capital letters.
 - Do not use cc: or bcc: fields unless the cc: or bcc: recipient is aware that you will be copying a mail to him/her and knows what action, if any, to take.
 - If you forward mails, state clearly what action you expect the recipient to take.
 - Only mark emails as important if they really are important.
- Maintenance:
 - Delete any email messages for which you do not need a copy, and set your email client to automatically empty your 'deleted items' on closing.

3.8 Personal Use

Agencies may permit employees to use email for occasional and incidental personal communications—the same way employees use phones—or may prohibit any personal use.

3.9 System Monitoring

Users expressly waive any right of privacy in anything they create, store, send or receive on the state's computer system. The state can, but is not obliged to, monitor emails without prior notification. If there is evidence that you are not adhering to the guidelines set out in this policy, the state reserves the right to take disciplinary action, including termination and/or legal action.

3.10 Disclaimer

The following disclaimer will be added to each outgoing email:

"This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the state. Finally, the recipient should check this email and any attachments for the presence of viruses. The State of Alabama accepts no liability for any damage caused by any virus transmitted by this email."

4. References

Alabama Internet Policy

Employee Internet and Network Security Guide

5. Declaration

I have read, understand and acknowledge receipt of the Email Policy. I will comply with the guidelines set out in this policy and understand that failure to do so might result in disciplinary or legal action.

Signature: _____ Date: _____

Printed Name: _____